UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

DAVID BRAMAN and MELISSA DUNN, individually, and on behalf of all others similarly situated, Plaintiffs, v. GPD HOLDINGS, LLC d/b/a CoinFlip, and CF PREFERRED LLC d/b/a Olliv, Defendants.	Case No.: **FIRST AMENDED CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiffs David Braman and Melissa Dunn, individually, and on behalf of all others similarly situated, bring this First Amended Class Action Complaint ("Complaint") against Defendants GPD Holdings, LLC d/b/a CoinFlip and CF Preferred d/b/a Olliv (collectively, "CoinFlip" or "Defendants"), to obtain damages, restitution, and injunctive relief for themselves and the Class, as defined below, from Defendants. Plaintiffs make the following allegations on information and belief, except as to his own actions, which are made on personal knowledge, the investigation of his counsel, and the facts that are a matter of public record.

I. NATURE OF THE ACTION

1. This class action arises out of the August 27, 2023 data breach involving CoinFlip, which led to the unauthorized disclosure of personally identifiable information of more than 36,000 of its customers ("Data Breach").

2. CoinFlip has a network 4,360 cryptocurrency ATM kiosks throughout the US, Puerto Rico and Canada, and offers a platform where over 400,000 of its customers can buy, sell,

trade or store cryptocurrencies.[1]

3. Unfortunately, CoinFlip failed to properly secure and safeguard the personally identifiable information provided by customers, including Plaintiffs and Class Members, including, without limitation, their full name, social security number, date of birth, state-issued driver's license, state-issued identification card, and passport number. ("PII").[2]

4. On information and belief, this Data Breach was engineered and targeted at accessing and exfiltrating the PII of Plaintiffs and Class Members in order for criminals to use that information in furtherance of theft, identity crimes, and fraud.

5. Defendants' failure to prevent and detect the Data Breach is particularly egregious considering the nature of its business, the PII they collected, and the myriad data breaches all over the country. The aggregate information acquired by cybercriminals in this Data Breach is particularly concerning considering that Defendants' customers provided PII which can be used to commit fraud against Plaintiffs and Class Members as well as steal their identities.

6. Plaintiffs bring this class action against CoinFlip to seek damages for himself and other similarly situated customers impacted by the Data Breach ("Class Members"), as well as other equitable relief, including, without limitation, injunctive relief designed to protect the sensitive information of Plaintiffs and other Class Members from further data breach incidents.

7. On or about October 23, 2023, CoinFlip filed a Notice of Data Breach ("Notice") with the Attorneys General of several states. The Notice states, "[o]n August 7, 2023, an unauthorized third-party utilized sophisticated social engineering tactics to access certain CoinFlip systems by compromising a CoinFlip employee's account."[3] It further states that CoinFlip discovered the Data Breach on August 8, 2023.[4] The Notice provided to the California Attorney

[1] Olliv, *About*, https://www.olliv.com/about (last accessed Nov. 3, 2023); CoinFlip, *About*, https://coinflip.tech/about (last accessed Nov 3, 2023).

[2] CoinFlip, *Notice of Data Breach*, https://oag.ca.gov/system/files/CoinFlip%20-%20California%20Draft%20Notice%20Letter%20to%20Individuals.pdf (last accessed Nov. 3, 2023).

[3] *Ibid.*

[4] *Ibid.*

General, for example, is as follows:

> **What Happened?**
>
> On August 7, 2023, an unauthorized third-party utilized sophisticated social engineering tactics to access certain CoinFlip systems by compromising a CoinFlip employee's account. Upon discovering this issue on August 8, 2023, we took immediate steps to both contain and thoroughly investigate this incident, including removing the unauthorized party from our environment. We also retained forensic consultants to assist with the investigation and analysis of the incident. Based on the investigation, which concluded on September 21, 2023, we determined that the unauthorized party had certain access to CoinFlip's systems for less than one day and during this time may have accessed and acquired certain of your data.
>
> **What Information Was Involved?**
>
> The personal information involved in this incident may have included your full name and tax identification number, which may also be your Social Security number, or your full name, date of birth, and either a driver's license, state-issued identification card, or passport number.[5]

8. As a result of Defendants' failure to prevent the Data Breach, or detect it during its occurrence thousands of CoinFlip customers across the United States are suffering and will continue to suffer real and imminent harm as a direct consequence of Defendants' conduct, which includes: (a) refusing to take adequate and reasonable measures to ensure its data systems were protected; (b) refusing to take available steps to prevent the breach from happening; (c) failing to adequately audit and monitor its employees; (d) failing to disclose to its customers the material fact that they did not have adequate computer systems and security practices to safeguard customers' PII; and (e) failing to provide timely and adequate notice of the Data Breach.

9. The injuries suffered by Plaintiffs and Class Members as a direct result of the Data Breach may include, inter alia:

a. Unauthorized charges on their payment card accounts;

b. Theft of their personal and financial information;

c. Costs associated with the detection and prevention of identity theft and

[5] *Ibid.*

unauthorized use of their financial accounts;

d. Loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit, including decreased credit scores and adverse credit notations;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempting to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

f. The present and continuing injury flowing from potential theft, fraud, and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted to CoinFlip for the sole purpose of using CoinFlip's services and with the mutual understanding that CoinFlip would safeguard Plaintiffs' and Class Members' PII against theft and not allow access to and misuse of their information by others;

h. Money paid to CoinFlip during the period of the Data Breach in that Plaintiffs and Class Members would not have used CoinFlip's services or products, or would have paid less for their services or products, had Defendants disclosed that they lacked adequate systems and procedures to reasonably safeguard customers' PII and had Plaintiffs and Class Members known that CoinFlip would not provide timely and accurate notice of the Data Breach; and,

i. Continued risk to their PII, which remains in the possession of CoinFlip, and which is subject to further breaches so long as CoinFlip continues to fail to undertake

appropriate and adequate measures to protect Plaintiffs' and Class Members' data in its possession.

10. Examples of the harms experienced by CoinFlip customers as a direct and foreseeable consequence of CoinFlip's conduct include the experiences of the representative Plaintiffs described below.

II. THE PARTIES

Plaintiff David Braman

11. Plaintiff David Braman is a citizen of the State of California and a is a resident of Riverside, California. Plaintiff Braman had his PII exfiltrated and compromised in the Data Breach announced by Defendants on or about October 23, 2023. Prior to the Data Breach, Plaintiff Braman used and paid for Defendants' services. To do so, Plaintiff Braman was required to provide Defendants with his PII. In making his decision to use Defendants' services, Plaintiff Braman reasonably expected that Defendants would safeguard his PII. Plaintiff Braman would not use Defendants' services, nor would have provided his PII, if he knew that the PII collected by Defendants would be at risk. Plaintiff Braman has suffered damages and remains at a significant risk now that his PII has been subject to an unauthorized disclosure.

Plaintiff Melissa Dunn

12. Plaintiff Melissa Dunn is a citizen of the State of California and a is a resident of Apple Valley, California. Plaintiff Dunn had her PII exfiltrated and compromised in the Data Breach announced by Defendants on or about October 23, 2023. Prior to the Data Breach, Plaintiff Dunn used and paid for Defendants' services. To do so, Plaintiff Dunn was required to provide Defendants with her PII. In making her decision to use Defendants' services, Plaintiff Dunn reasonably expected that Defendants would safeguard her PII. Plaintiff Dunn would not use Defendants' services, nor would have provided her PII, if she knew that the PII collected by Defendants would be at risk. Plaintiff Dunn has suffered damages and remains at a significant risk now that her PII has been subject to an unauthorized disclosure

Defendants

13. Defendant GPD Holdings, LLC d/b/a CoinFlip is a privately held corporation incorporated in the State of Delaware, which includes COINFLIP LLC as a sole manager. Both COINFLIP LLC and Defendant GPD Holdings, LLC d/b/a CoinFlip's shared headquarters are located at 433 W. Van Buren St., Suite 1050N, Chicago, IL 60607. All of Plaintiffs' claims stated herein are asserted against Defendants and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

14. Defendant CF Preferred LLC d/b/a Olliv is a privately held corporation incorporated in the State of Delaware, which includes COINFLIP LLC as a sole manager. Both COINFLIP LLC and Defendant CF Preferred d/b/a Olliv's shared headquarters located at 433 W. Van Buren St., Suite 1050N, Chicago, IL 60607. All of Plaintiffs' claims stated herein are asserted against Defendants and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

15. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. §1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendants to establish minimal diversity.

16. This Court has personal jurisdiction over Defendants because Defendants and/or their parents or affiliates are headquartered in this District and Defendants conduct substantial business in Illinois and this District through its headquarter, offices, parents, and affiliates.

17. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendants and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

18. CoinFlip operates a network of 4,360 cryptocurrency ATM kiosks throughout the

US, Puerto Rico and Canada, and offers a platform where over 400,000 of its customers can buy, sell, trade or store cryptocurrencies.6 CoinFlip is a privately held company with corporate headquarters in Chicago, Illinois.

19. To use Defendants' services, a customer must provide certain PII.

20. When they provided their PII to Defendants, Plaintiffs and Class Members relied on Defendants (a large, sophisticated cryptocurrency enterprise) to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

21. Defendants had a duty to take reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to unauthorized third parties. This duty is inherent in the nature of the exchange of the highly sensitive PII at issue here, particularly where digital transactions are involved.

22. Defendants also recognized and voluntarily adopted additional duties to protect PII in their Privacy Policy which has been publicly posted to the internet.7 In their Privacy Policy, Defendants also say they "have put in place commercially reasonable administrative, technical, and physical measures in an effort to prevent unauthorized access to or disclosure of personal data, and [] take reasonable steps to secure and safeguard this data against loss, theft, and unauthorized use, disclosure, or modification."8

23. Despite these duties and promises, Defendants allowed data thieves to infiltrate its data storage systems and steal the PII of thousands of its customers. Specifically, hackers used social engineering tactics to access Defendants' data storage systems, instead of using highly technical hacking methods that require advanced knowledge of computer programing and network systems engineering.

---

[6] Olliv, *About*, https://www.olliv.com/about (last accessed Nov. 3, 2023); CoinFlip, *About*, https://coinflip.tech/about (last accessed Nov 3, 2023).

[7] Olliv, *Privacy Policy*, https://www.olliv.com/privacy-policy (last accessed Nov. 3, 2023); CoinFlip, *Privacy Policy*, https://coinflip.tech/terms/privacy-policy (last accessed Nov 3, 2023).

[8] *Id.*

The Data Breach was foreseeable

24. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.9

25. In light of recent high profile data breaches at other industry leading companies, including Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendants knew or should have known that the PII that it collected and maintained would be targeted by cybercriminals.

26. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

27. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgment of its duties to keep PII confidential and secure, Defendants failed to take appropriate steps to protect the PII of Plaintiffs and the Class from being compromised.

The Data Breach

28. On or about October 23, 2023, Defendants notified various state Attorneys General, as well as Plaintiffs and Class Members, that, on August 8, 2023, Defendants discovered "an unauthorized third-party utilized sophisticated social engineering tactics to access certain CoinFlip systems by compromising a CoinFlip employee's account."10

29. The Notice informed Plaintiffs and Class Members that "the investigation, which

---

[9] Bree Fowler, *Data breaches break record in 2021*, CNET (Nov. 3, 2023), https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/#:~:text=The%20number%20of%20reported%20data%20breaches%20jumped%2068%20percent%20last,of%201%2C506%20set%20in%202017.

[10] CoinFlip, *Notice of Data Breach*, https://oag.ca.gov/system/files/CoinFlip%20-%20California%20Draft%20Notice%20Letter%20to%20Individuals.pdf (last accessed Nov. 3, 2023).

concluded on September 21, 2023, [] determined that [an] unauthorized party had certain access to CoinFlip's systems for less than one day and during this time may have accessed and acquired certain of your data."11 This information included full name, social security number, date of birth, state-issued driver's license, state-issued identification card, and passport number.12

30. Despite Defendants' promises that it: (i) would not disclose consumers' PII to unauthorized third parties; and (ii) would protect consumers' PII with adequate security measures, it appears that Defendants did not even implement basic security measures.

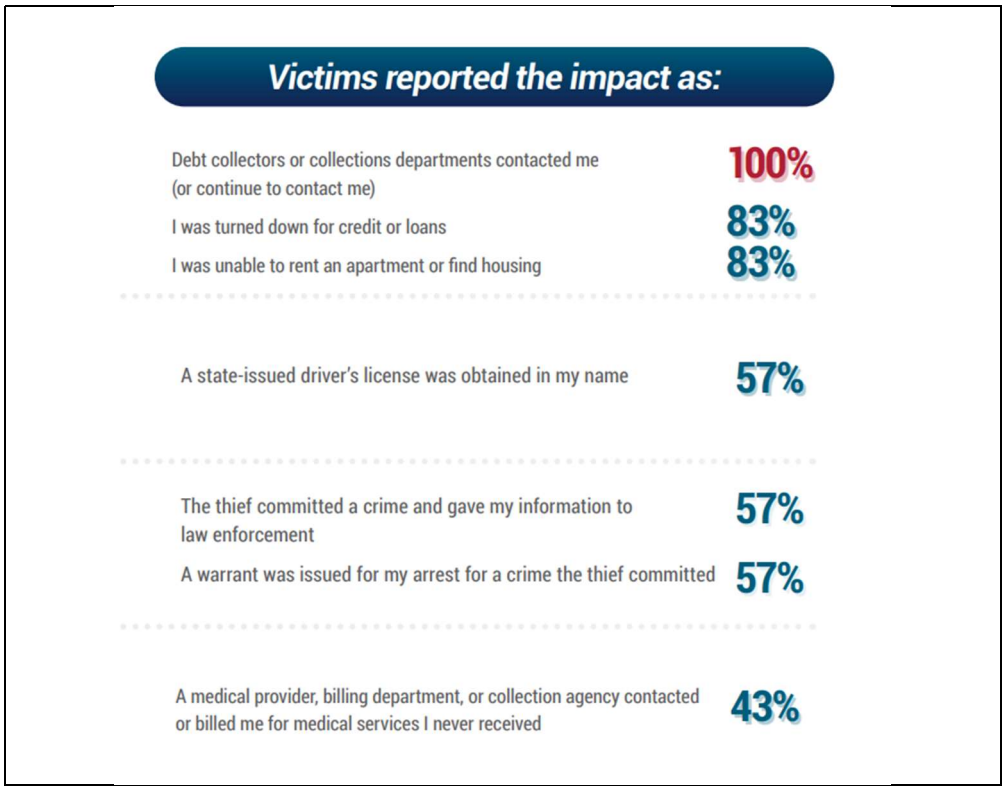
Securing PII and Preventing Breaches

31. Given CoinFlip's nature of business, it should have been even more aware and taken further precautions to secure PII and other PII. Since the Data Breach was accomplished by social engineering, on information and belief, CoinFlip did not hold security awareness trainings, simulated social engineering attempts, nor implemented multi-factor authentication.

32. The financial fraud suffered by Plaintiffs and other customers demonstrates that Defendants chose not to invest in the technology to make its customers' data more secure; failed to install updates, patches, and malware protection or to install them in a timely manner to protect against a data security breach; and/or failed to provide sufficient control of employee credentials and access to computer systems to prevent a security breach and/or theft of PII.

33. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personally identifiable information :[13]

[11] *Id.*
[12] *Id.*
[13] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, https://www.idtheftcenter.org/wp-content/uploads/2021/09/ITRC_2021_Consumer_Aftermath_Report.pdf (last visited Nov. 15, 2022)



34. Plaintiffs and Class Members have experienced one or more of these harms as a result of the Data Breach.

35. Furthermore, theft of PII is also gravely serious. PII is a valuable property right. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

36. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[14]

[14] U.S. GOV'T ACCOUNTABILITY OFF., GAO 07737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, 12 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

37. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

38. There is a strong probability that entire batches of stolen PII have been dumped on the black market or are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud for many years into the future. Thus, Plaintiffs and Class Members must vigilantly monitor their financial accounts for many years to come.

39. Plaintiffs and Class Members have and will continue to suffer injuries as a direct result of the Data Breach. In addition to fraudulent charges and damage to their credit, many victims spent substantial time and expense relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Removing withdrawal and purchase limits on compromised accounts;

f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

g. Spending time on the phone with or at the financial institution to dispute fraudulent charges;

h. Resetting automatic billing instructions; and

i. Paying late fees and declined payment fees imposed as a result of failed automatic payments.

40. Plaintiffs and Class Members have been damaged by the compromise of their PII in the Data Breach.

41. Plaintiffs' and Class Members' PII was compromised as a direct and proximate result of the Data Breach.

42. As a direct and proximate result of the Data Breach, Plaintiffs' PII was exfiltrated and is in the hands of identity thieves and criminals, as evidenced by the fraud perpetrated against Plaintiffs and Class Members.

43. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have been placed at an immediate and continuing increased risk of harm from fraud. Plaintiffs and Class Members now have to take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing, or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

44. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

45. Plaintiffs and Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

46. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. The implied contractual bargain entered into between Plaintiffs and Defendants included Defendants' contractual obligation to provide adequate data security, which Defendants failed to provide. Thus, Plaintiffs and the Class Members did not get what they paid for.

47. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time monitoring their financial accounts and records for misuse.

48. Plaintiffs and Class Members have suffered, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. Trespass, damage to and theft of their personal property including PII;

b. Improper disclosure of their PII property;

c. The present and continuing injury flowing from potential fraud and identity theft posed by customers' PII being placed in the hands of criminals;

d. Damages flowing from Defendants' untimely and inadequate notification of the Data Breach;

e. Loss of privacy suffered as a result of the Data Breach;

f. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

g. Ascertainable losses in the form of deprivation of the value of customers' PII for which there is a well-established and quantifiable national and international market; and,

h. The loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money customers were permitted to obtain from their accounts.

49. The substantial delay in providing notice of the Data Breach deprived Plaintiffs and the Class Members of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach. As a result of Defendants' delay in notifying consumers of the Data Breach, the risk of fraud for Plaintiffs and Class Members was and has been driven even higher.

Value of Personal Identifiable Information

50. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.15 Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.16 Criminals can also purchase access to entire company data breaches from $900 to $4,500.

51. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.17 In fact, the data marketplace is so

[15] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[16] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/

[17] David Lazarus, *Column: Shadowy data brokers make the most of their invisibility cloak*, LOS ANGELES TIMES (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.18 Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.19

52. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its acquisition by cybercriminals. This transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the PII is likely readily available to others, and the rarity of the PII has been destroyed, thereby causing additional loss of value.

53. The fraudulent activity resulting from the Data Breach may not come to light for years and Plaintiffs and Class Members face a lifetime risk of fraud and identity theft as a result of the Data Breach.

54. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[20]

55. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, particularly given the sensitive nature of their cryptocurrency transactions, and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the

[18] *See* Data Coup, https://datacoup.com/ (last visited on Nov. 3, 2023).

[19] Nielsen, *Frequently Asked Questions, Nielsen Computer & Mobile Panel*, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Nov. 3, 2023).

[20] U.S. Gov't Accountability Off., GAO 07737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

significant costs and risks that would be imposed on Plaintiffs and Class Members as a result of a breach.

56. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

57. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' storage platform, amounting to tens or hundreds of thousands of individuals' detailed, PII and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

58. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures, and failure to adequately investigate, monitor, and audit its employees, to protect the II of Plaintiffs and Class Members.

Plaintiffs' Experiences

59. Plaintiffs both suffered actual injury from having their PII compromised and/or stolen as a result of the Data Breach.

60. Plaintiffs suffered actual injury and damages in paying money to and using services from Defendants that they would not have paid had Defendants disclosed that they lacked computer systems and data security practices adequate to safeguard customers' personal and financial information and had Defendants provided timely and accurate notice of the Data Breach. Specifically, Plaintiffs paid transaction fees and network fees to use Defendants services.

61. Plaintiffs suffered actual injury in the form of damages to and diminution in the value of their PII – a form of intangible property that Plaintiffs entrusted to Defendants for the purpose using Defendants' service, and which was compromised in, and as a result of, the Data Breach.

62. Plaintiffs suffer present and continuing injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by their personal and financial

information being placed in the hands of criminals who have already misused such information stolen in the Data Breach.

63. Plaintiffs have a continuing interest in ensuring that their PII, which remains in the possession of Defendants, is protected, and safeguarded from future breaches.

64. As a result of the Data Breach, Plaintiffs made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services offered by Defendants. Plaintiffs have spent several hours dealing with the Data Breach, valuable time Plaintiffs otherwise would have spent on other activities.

65. As a result of the Data Breach, Plaintiffs have suffered anxiety as a result of the release of their PII, which they believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using their PII for purposes of identity crimes, fraud, and theft. Plaintiffs are very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

66. Plaintiffs suffered actual injury from having their PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of their PII, a form of property that Defendants obtained from Plaintiff; (b) violation of their privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

67. As a result of the Data Breach, Plaintiffs anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiffs are at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Defendants Failed to Comply with Recognized Security Standards

68. Despite the prevalence of public announcements of data breach and data security compromises, and despite Defendants' own acknowledgment of its duties to keep PII private and

secure, Defendants failed to take appropriate steps to protect the PII of Plaintiffs and the Class from being compromised.

69. Defendants had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite their obligation to protect such information. Accordingly, Defendants breached their common law, statutory, and other duties owed to Plaintiffs and Class Members.

70. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs;

j. Monitoring for server requests from TOR exit nodes; and

k. Monitoring and auditing the programming of its websites.

l. Upon information and belief, Defendants failed to comply with one or more of these standards.

CoinFlip Failed to Comply with FTC Guidelines

71. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other

things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

72. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making.

73. The FTC has brought well-publicized enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. This includes the FTC's enforcement action against Equifax following a massive data breach involving the personal and financial information of 147 million Americans.

74. In 2016, the FTC updated its publication, "Protecting Personal Information: A Guide for Business," which established cyber-security guidelines for businesses. There, the FTC advised that businesses should protect the PII that they keep by following some minimum standards related to data security, including, among others:

a. Encrypting information stored on computer networks;

b. Identifying network vulnerabilities;

c. Implementing policies to update and correct any security problems;

d. Implementing multifactor authentication;

e. Simulating social engineering attacks;

f. Utilizing an intrusion detection systems;

g. Monitor all incoming traffic for suspicious activity indicating someone is attempting to hack the system;

h. Watching for large amounts of data being transmitted from the system;

i. Developing a response plan ready in the event of a breach;

j. Limiting employee and vendor access to sensitive data;

k. Requiting complex passwords to be used on networks;

l. Utilizing industry-tested methods for security;

m. Verifying that third-party service providers have implemented reasonable security measures;

n. Educating and training employees on data security practices;

o. Implementing multi-layer security including firewalls, anti-virus, and anti-malware software; and

p. Implementing multi-factor authentication.

75. Upon information and belief, Defendants failed to implement or adequately implement at least one of these fundamental data security practices.

76. Defendants' failure constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

V. CLASS ACTION ALLEGATIONS

77. Plaintiffs bring this nationwide class action on behalf of themselves, and all others similarly situated, under Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

78. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> "All persons Defendants identified as being among those individuals impacted by the Data Breach, including all persons who were sent a Notice of the Data Breach."

79. Said definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court

80. The California Subclass which Plaintiffs seek to represent comprises:

> "All persons residing in California Defendants identified as being among those individuals impacted by the Data Breach, including those who were sent a Notice of the Data Breach" (the "California Subclass").

81. Said definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

82. Excluded from the Class are Defendants' officers and directors; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families, and members of their staff.

83. Plaintiffs reserves the right to amend or modify the Class definition and/or create additional subclasses as this case progresses.

84. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of at least 36,646 current and former customers of Defendants whose PII was compromised in Data Breach.21

85. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' PII;

b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendants owed a duty to Class Members to safeguard their PII;

f. Whether Defendants breached its duty to Class Members to safeguard their PII;

[21] Maine Attorney General, *Data Breach Notifications: GPD Holdings LLC d/b/a CoinFlip.*, https://apps.web.maine.gov/online/aeviewer/ME/40/ebd8789c-74d3-4add-9c77-b45294ca037b.shtml (last visited Nov. 3, 2023).

g. Whether Defendants knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendants should have discovered the Data Breach sooner;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

j. Whether Defendants' conduct was negligent;

k. Whether Defendants' acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

l. Whether Defendants breach implied or express contracts with Plaintiffs and Class Members;

m. Whether Defendants was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class Members;

n. Whether Defendants failed to provide notice of the Data Breach in a timely manner, and;

o. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

86. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach.

87. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class and have no interests antagonistic to those of other Class Members. Plaintiffs' counsel are competent and experienced in litigating class actions.

88. Predominance. Defendants have engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable

advantages of judicial economy.

89. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

90. Defendants have acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

COUNT I

VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW,

CAL. BUS. & PROF. CODE § 17200 et seq.

(On Behalf of the California Subclass and Nationwide Class)

91. Plaintiffs, individually and on behalf of the Class, herein repeat, reallege and fully incorporate all allegations in all preceding paragraphs.

A. "Unfair" Prong

92. Under California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 et seq., a challenged activity is "unfair" when "any injury it causes outweighs any benefits provided to consumers and the injury is one that the consumers themselves could not reasonably avoid." *Camacho v. Auto Club of Southern California*, 142 Cal. App. 4th 1394, 1403 (2006).

93. Defendants' conduct as alleged herein does not confer any benefit to consumers. It is especially questionable why Defendants would continue to store individuals' data longer than

necessary. Mishandling this data and a failure to archive and purge this unnecessary data shows blatant disregard for consumer's privacy and security.

94. Defendants did not need to collect the PII from its consumers to allow consumers' enhanced experiences of the products or services. It did so to track and target its customers and monetize the use of the data to enhance its profits. Defendants utterly misused this PII and other data.

95. Defendants' conduct as alleged herein causes injuries to consumers, who do not receive a service consistent with their reasonable expectations.

96. Defendants' conduct as alleged herein causes injuries to consumers who entrusted Defendants with their PII and whose PII was leaked as a result of Defendants' unlawful conduct.

97. Defendants' failure to implement and maintain reasonable security measures was also contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, California's Consumer Records Act, Cal. Civ. Code §1798.81.5, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100.

98. Consumers cannot avoid any of the injuries caused by Defendants' conduct as alleged herein.

99. The injuries caused by Defendants' conduct as alleged herein outweigh any benefits, and thus unfair.

100. Defendants' conduct, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes an unfair business practice within the meaning of Cal. Bus. & Prof. Code § 17200.

101. Defendants could have furthered its legitimate business interests in ways other than by unfair conduct.

102. Defendants' conduct threatens consumers by exposing consumers' PII to hackers. Defendants' conduct also threatens other companies, large and small, who play by the rules. Defendants' conduct stifles competition and has a negative impact on the marketplace and reduces

consumer choice.

103. All of the conduct alleged herein occurs and continues to occur in Defendants' business. Defendants' wrongful conduct is part of a pattern or generalized course of conduct.

104. Pursuant to Cal. Bus. & Prof. Code § 17203, Plaintiffs and the Class seek an order of this Court enjoining Defendants from continuing to engage, use, or employ its unfair business practices.

105. Plaintiffs and the Class have suffered injury-in-fact and have lost money or property as a result of Defendants' unfair conduct. Plaintiffs relied on and made their decision to use Defendants' services in part based on Defendants' representations regarding their security measures and trusted that Defendants would keep his PII safe and secure. Plaintiffs accordingly provided their PII to Defendants reasonably believing and expecting that his PII would be safe and secure. Plaintiffs paid an unwarranted premium for the purchased services. Specifically, Plaintiffs paid for services advertised as secure when Defendants in fact failed to institute adequate security measures and neglected vulnerabilities that led to a data breach. Plaintiffs and the Class would not have purchased the services, or would not have given Defendant their PII, had they known that their PII was vulnerable to a data breach. Likewise, Plaintiffs and the Members of the Class seek an order mandating that Defendants implement adequate security practices to protect consumers' PII. Additionally, Plaintiffs and the Members of the Class seek and request an order awarding Plaintiffs and the Class restitution of the money wrongfully acquired by Defendants by means of Defendants' unfair and unlawful practices.

B. "Fraudulent" Prong

106. Cal. Bus. & Prof. Code § 17200, et seq. considers conduct fraudulent and prohibits said conduct if it is likely to deceive members of the public. *Bank of the West v. Superior Court*, 2 Cal. 4th 1254, 1267 (1992).

107. Defendants' advertising and representations that they adequately protect consumer's PII is likely to deceive members of the public into believing that CoinFlip can be entrusted with their PII, and that PII gathered by CoinFlip is not in danger of being compromised.

108. Defendants' representations about their services, as alleged in the preceding paragraphs, are false, deceptive, misleading, and unreasonable and constitutes fraudulent conduct.

109. Defendants knew or should have known of its fraudulent conduct.

110. As alleged in the preceding paragraphs, the material misrepresentations by Defendants detailed above constitute a fraudulent business practice in violation of Cal. Bus. & Prof. Code § 17200 et seq.

111. Defendants could have implemented robust security measures to prevent the data breach but failed to do so.

112. Defendants' wrongful conduct is part of a pattern or generalized course of conduct.

113. Pursuant to Cal. Bus. & Prof. Code § 17203, Plaintiffs and the Class seek an order of this Court enjoining Defendants from continuing to engage, use, or employ its practice of false and deceptive advertising about the strength or adequacy of its security systems.

114. Likewise, Plaintiffs and the Class seek an order requiring Defendants to disclose such misrepresentations.

115. Plaintiffs and the Class have suffered injury in fact and have lost money as a result of Defendants' fraudulent conduct. Plaintiffs paid an unwarranted premium for services. Plaintiffs would not have used the services, if he had known that his use would put his PII at risk.

116. Pursuant to Cal. Bus. & Prof. Code § 17203, Plaintiffs and the Class seek an order of this Court compelling Defendants to implement adequate safeguards to protect consumer's PII retained by Defendants. This includes, but is not limited to: improving security systems, deleting data that no longer needs to be retained by Defendants, archiving that data on secure servers, and notifying all affected consumers in a timely manner.

C. "Unlawful" Prong

117. Cal. Bus. & Prof. Code § 17200, et seq., identifies violations of any state or federal law as "unlawful practices that the unfair competition law makes independently actionable." *Velazquez v. GMAC Mortg. Corp.*, 605 F. Supp. 2d 1049, 1068 (C.D. Cal. 2008).

118. Defendants' unlawful conduct, as alleged in the preceding paragraphs, violates Cal.

Bus. & Prof. Code § 1750 et seq.

119. Defendants' conduct, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes unlawful conduct.

120. Defendants have engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, et seq., the FTC Act, 15 U.S.C. § 45, and California common law. Defendants failed to notify all of its affected customers regarding said breach, failed to take reasonable security measures, or comply with the FTC Act, and California common law.

121. Defendants knew or should have known of its unlawful conduct.

122. As alleged in the preceding paragraphs, the misrepresentations by Defendants detailed above constitute an unlawful business practice within the meaning of Cal. Bus. & Prof. Code §17200.

123. Defendants could have furthered its legitimate business interests in ways other than by its unlawful conduct.

124. All of the conduct alleged herein occurs and continues to occur in Defendants' business. Defendants' unlawful conduct is part of a pattern or generalized course of conduct.

125. Pursuant to Cal. Bus. & Prof. Code § 17203, Plaintiffs and the Class seek an order of this Court enjoining Defendants from continuing to engage, use, or employ its unlawful business practices.

126. Plaintiffs and the Class have suffered injury-in-fact and have lost money or property as a result of Defendants' unfair conduct. Plaintiffs paid an unwarranted premium for services. Specifically, Plaintiffs paid for services advertised as secure when Defendants in fact failed to institute adequate security measures and neglected vulnerabilities that led to a data breach. Plaintiffs and the Class would not have purchased the products and services, or would not have given Defendants his PII, had they known that their PII was vulnerable to a data breach. Likewise,

Plaintiffs and the members of the Class seek an order mandating that Defendants implement adequate security practices to protect consumers' PII. Additionally, Plaintiffs and the members of the Class seek and request an order awarding Plaintiffs and the Class restitution of the money wrongfully acquired by Defendants by means of Defendants' unfair and unlawful practices.

COUNT II

VIOLATION OF CALIFORNIA'S CONSUMER LEGAL REMEDIES ACT,

CAL. CIV. CODE § 1750, et seq.

(On Behalf of the California Subclass)

127. Plaintiffs repeat and re-alleges the allegations set forth in the preceding paragraphs and incorporates the same as if set forth herein at length.

128. The CLRA prohibits certain "unfair methods of competition and unfair or deceptive acts or practices" in connection with a sale of services.

129. Defendants' unlawful conduct described herein was intended to increase sales to the consuming public and violated and continues to violate §§ 1770(a)(5), (a)(7), and (a)(9) of the CLRA by representing that the products and services have characteristics and benefits which they do not have.

130. Defendants fraudulently deceived Plaintiffs and the California Subclass by representing that its services have certain characteristics, benefits, and qualities which they do not have, namely data protection and security. In doing so, Defendants intentionally misrepresented and concealed material facts from Plaintiffs and the California Subclass, specifically by advertising secure technology when Defendants in fact failed to institute adequate security measures and neglected system vulnerabilities that led to a data breach. Said misrepresentations and concealment were done with the intention of deceiving Plaintiffs and the California Subclass and depriving them of their legal rights and money.

131. Defendants' claims about the products and services led and continues to lead consumers like Plaintiffs to reasonably believe that Defendants have implemented adequate data security measures when Defendants in fact neglected system vulnerabilities that led to a data

breach and enabled hackers to access consumers' PII.

132. Defendants knew or should have known that adequate security measures were not in place and that consumers' PII was vulnerable to a data breach.

133. Plaintiffs and the California Subclass have suffered injury in fact as a result of and in reliance upon Defendants' false representations.

134. Plaintiffs and the California Subclass would not have purchased the products or used the services or would have paid significantly less for the products and services, had they known that their PII was vulnerable to a data breach.

135. Defendants' actions as described herein were done with conscious disregard of Plaintiffs' rights, and Defendants was wanton and malicious in its concealment of the same.

136. Plaintiffs and the California Subclass have suffered injury in fact and have lost money as a result of Defendants' unfair, unlawful, and fraudulent conduct. Specifically, Plaintiffs paid for services advertised as secure, and consequentially entrusted Defendants with their PII, when Defendants in fact failed to institute adequate security measures and neglected vulnerabilities that led to a data breach. Specifically, Plaintiffs paid for use of Coinflip's network in the form of network fees which CoinFlip charges at a minimum of $1.99. Plaintiffs and the California Subclass would not have purchased the products and services, or would not have provided Defendants with their PII, had they known that their PII was vulnerable to a data breach.

137. Defendants should be compelled to implement adequate security practices to protect consumers' PII. Additionally, Plaintiffs and the members of the California Subclass lost money as a result of Defendant's unlawful practices.

138. At this time, Plaintiffs seek injunctive relief under the CLRA pursuant to Cal. Civ. Code § 1782(d); but anticipates needing to amend the complaint and seek restitution.

COUNT III

(PENDING EXHAUSTION OF 30-DAY CURE PERIOD)

VIOLATION OF CALIFORNIA'S CONSUMER PRIVACY ACT ("CCPA"),

CAL. CIV. CODE § 1798.150 et seq.

(On Behalf of the California Subclass)

139. Plaintiffs repeat and re-allege the allegations set forth in the preceding paragraphs, and incorporates the same as if set forth herein at length.

140. Defendants are corporations organized or operated for the profit or financial benefit of its owners with annual gross revenues in excess of $25,000,000.

141. Defendants collects consumers' personal information as defined in Cal. Civ. Code § 1798.140.

142. Defendants violated § 1798.150 of the CCPA by failing to prevent Plaintiffs' and the California Subclass Members' nonencrypted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendants' violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

143. Defendants have a duty to implement and maintain reasonable security procedures and practices to protect Plaintiffs' and California Subclass Members' PII. As detailed herein, Defendants failed to do so.

144. As a direct and proximate result of Defendants' acts, Plaintiffs' and California Subclass Members' PII, as defined in Cal. Civ. Code § 1798.81.5(d)(1)(A), including full name, social security number, date of birth, state-issued driver's license, state-issued identification card, and passport number, was subjected to unauthorized access and exfiltration, theft, or disclosure.

145. Plaintiffs and California Subclass Members seek injunctive or other equitable relief to ensure Defendants hereinafter adequately safeguards customers' PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendants continues to hold customers' PII, including Plaintiffs and California Subclass Members' PII. Plaintiffs and California Subclass Members have an interest in ensuring that their PII is reasonably protected, and Defendants have demonstrated a pattern of failing to adequately safeguard this information, as evidenced by its Data Breach.

146. As described herein, an actual controversy has arisen and now exists as to whether Defendants implemented and maintained reasonable security procedures and practices appropriate

to the nature of the information to protect the PII under the CCPA.

147. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendants and third parties with similar inadequate security measures.

148. Plaintiffs and the California Subclass seek actual pecuniary damages, including actual financial losses resulting from the unlawful data breach.

149. On November 3, 2023, Plaintiffs' counsel sent a notice letter to Defendant's registered address. Assuming Defendants cannot cure the Data Breach within 30 days, and Plaintiffs believes such cure is not possible under these facts and circumstances, then Plaintiffs intend to promptly amend this complaint to seek actual damages and statutory damages of $750 per customer record subject to the Data Breach on behalf of the California Subclass as permitted by the CCPA.

COUNT IV

Negligence

(On behalf of Plaintiffs and Class Members)

150. Plaintiffs repeat and reallege all of the allegations contained above and incorporates the same as if set forth herein at length.

151. Defendants solicited and gathered the PII of Plaintiffs and Class Members to facilitate cryptocurrency transactions.

152. Defendants knew, or should have known, of the risks inherent in collecting the PII of Plaintiffs and the Class Members and the importance of adequate security. Defendants also knew about numerous, well-publicized data breaches involving similar organizations.

153. Defendants owed duties of care to Plaintiffs and the Class Members whose PII was entrusted to it. Defendants' duties included the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting PII in its possession;

b. To exercise reasonable care in selecting its employees and monitoring and auditing

their data security practices ensuring compliance with legal and industry standards and obligations;

c. To protect customers' PII using reasonable and adequate security procedures and systems that are compliant and consistent with industry-standard practices;

d. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

e. To promptly notify Plaintiffs and Class Members of the Data Breach.

154. By collecting this data and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard its computer property, to prevent disclosure of PII, and to safeguard the PII from theft. Defendants' duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in case of a data breach.

155. Defendants' duty of care extended to ensuring that any employees hired and that had exposure to the PII of Plaintiffs and Class Members would implement adequate measures to prevent and detect cyber intrusions.

156. Because Defendants knew that a breach of its systems would damage thousands of its customers, including Plaintiffs and Class Members, they had a duty to adequately protect their PII.

157. Defendants owed a duty of care not to subject Plaintiffs and the Class Members to an unreasonable risk of harm because they were the foreseeable and probable victims of any inadequate security practices.

158. Defendants had a duty to implement, maintain, and ensure reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' PII.

Defendants knew, or should have known, that its computer systems and security practices did not adequately safeguard the PII of Plaintiffs and the Class Members.

159. Defendants breached its duties of care by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII of Plaintiffs and the

Class Members.

160. Defendants breached its duties of care by failing to provide prompt notice of the data breach to the persons whose PII was compromised.

161. Defendants acted with reckless disregard for the security of the PII of Plaintiffs and the Class Members because Defendants knew or should have known that its computer systems and data security practices were not adequate to safeguard the PII that that it collected, which hackers targeted in the Data Breach.

162. Defendants acted with reckless disregard for the rights of Plaintiffs and the Class Members by failing to provide prompt and adequate notice of the Data Breach so that they could take measures to protect themselves from damages caused by the fraudulent use the PII compromised in the Data Breach.

163. Defendants had a special relationship with Plaintiffs and the Class Members. Plaintiffs' and the Class Members' willingness to entrust Defendants with their PII was predicated on the mutual understanding that Defendants would implement adequate security precautions. Moreover, Defendants were in an exclusive position to protect its systems (and the PII) from attack. Plaintiffs and Class Members relied on Defendants to protect their PII.

164. Defendants' own conduct also created a foreseeable risk of harm to Plaintiffs and Class Members and their PII. Defendants' misconduct included failing to:

a. Secure its website and internal systems;

b. Audit and monitor its employees;

c. Comply with industry standard security practices;

d. Encrypt PII at the point-of-transaction and during transit;

e. Employ adequate network segmentation;

f. Implement adequate system and event monitoring;

g. Install updates and patches in a timely manner; and

h. Implement the systems, policies, and procedures necessary to prevent this type of data breach.

165. Defendants also had independent duties under the FTC Act and state laws that required it to reasonably safeguard Plaintiffs' and the Class Members' PII and promptly notify them about the Data Breach.

166. Defendants breached the duties it owed to Plaintiffs and Class Members in numerous ways, including:

a. By creating a foreseeable risk of harm through the misconduct previously described;

b. By failing to implement adequate security systems, protocols, and practices sufficient to protect their PII both before and after learning of the Data Breach;

c. By failing to comply with the minimum industry data security standards during the period of the Data Breach, and

d. By failing to timely and accurately disclose that the PII of Plaintiffs and the Class had been improperly acquired or accessed.

167. But for Defendants' wrongful and negligent breach of the duties it owed Plaintiffs and the Class Members, their personal and financial information either would not have been compromised or they would have been able to prevent some or all of their damages.

168. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and the Class Members have suffered damages and are at imminent risk of further harm.

169. The injury and harm that Plaintiffs and Class Members suffered (as alleged above) was reasonably foreseeable.

170. The injury and harm that Plaintiffs and Class Members suffered (as alleged above) was the direct and proximate result of Defendants' negligent conduct.

171. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT V

Intentional Misrepresentation

(On Behalf of Plaintiffs and Class Members)

172. Plaintiffs repeat and reallege all of the allegations contained above and incorporate the same as if set forth herein at length.

173. Defendants have represented, through its privacy policy, that Defendant "safeguards" all information provided by consumers, particularly "personal data."[22]

174. Defendants in fact misrepresented the security of its services and products, failed to institute adequate security measures, and neglected vulnerabilities that led to a data breach of sensitive, personal information.

175. Defendants' misrepresentations regarding its security systems are material to a reasonable consumer, as they relate to the privacy of consumers' PII. A reasonable consumer would assign importance to such representations and would be induced to act thereon in making his or her decision to use Defendants' services.

176. At all relevant times when such misrepresentations were made, Defendants knew or should have known that the representations were misleading.

177. Defendants intended for Plaintiffs and the Class to rely on the representations of its security systems, as evidenced by Defendants' intentional marketing of safe and secure services.

178. Plaintiffs and members of the Class reasonably and justifiably relied on Defendants' intentional misrepresentations when using its services, and had they known the truth, they would not have used the services or would not have given Defendants their PII.

179. Defendants were negligent in its representations that it would provide the highest level of security for consumers.

180. As a direct and proximate result of Defendants' intentional misrepresentations, Plaintiffs and members of the Class have suffered injury in fact.

COUNT VI

Breach of Express Contract

(On Behalf of Plaintiffs and the Nationwide Class)

[22] Olliv, *Privacy Policy*, https://www.olliv.com/privacy-policy (last accessed Nov. 3, 2023); CoinFlip, *Privacy Policy*, https://coinflip.tech/terms/privacy-policy (last accessed Nov 3, 2023).

181. Plaintiffs incorporate by reference all other allegations in the Complaint as if fully set forth herein.

182. Plaintiffs and Class Members allege that they were the express, foreseeable, and intended beneficiaries of valid and enforceable express contracts between Defendants and its former and current clients, contract(s) that (upon information and belief) include obligations to keep sensitive PII private and secure.

183. Upon information and belief, these contracts included promises made by Defendants that expressed and/or manifested intent that the contracts were made to primarily and directly benefit Plaintiffs and the Class (all customers entering into the contracts), as Defendants' business is for services for Plaintiffs and the Class, but also safeguarding the PII entrusted to Defendants in the process of providing these services.

184. Upon information and belief, Defendants' representations required Defendants to implement the necessary security measures to protect Plaintiffs' and Class Members' PII.

185. Defendants materially breached their contractual obligation to protect the PII of Plaintiffs and Class Members when the information was accessed and exfiltrated by unauthorized personnel as part of the Data Breach.

186. The Data Breach was a reasonably foreseeable consequence of Defendants' actions in breach of these contracts.

187. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure of their PII, the loss of control of their PII, the present risk of suffering additional damages, and out-of-pocket expenses.

188. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

COUNT VII

Breach of Implied Contract

(On behalf of Plaintiffs and Class Members)

189. Plaintiffs repeat and reallege all of the allegations contained above and incorporate the same as if set forth herein at length.

190. When Plaintiffs and Class Members provided their PII to Defendants in making transactions on Defendants' systems, they entered into implied contracts under which Defendants agreed to protect their PII and timely notify them in the event of a data breach.

191. Defendants invited its customers, including Plaintiffs and the Class, to make cryptocurrency transactions in order to increase sales by making the transactions more convenient.

192. An implicit part of the offer was that Defendants would safeguard their PII using reasonable or industry-standard means and would timely notify Plaintiffs and the Class in the event of a data breach.

193. Defendants also affirmatively represented in its Privacy Policy that it protected the PII of Plaintiffs and the Class in several ways, as described above.

194. Based on the implicit understanding and also on Defendants' representations, Plaintiffs and the Class accepted the offers and provided Defendants with their PII by making cryptocurrency transactions during the period of the Data Breach.

195. Defendants manifested its intent to enter into an implied contract that included a contractual obligation to reasonably protect Plaintiffs' and Class Members' PII through, among other things, its Privacy Notice.

196. Defendants further demonstrated an intent to safeguard the PII of Plaintiffs and Class Members through its conduct. No reasonable person would provide sensitive, non-public information without the implicit understanding that the organization would maintain that information as confidential.

197. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations and were consistent with industry standards.

198. Plaintiffs and Class Members would not have provided their PII to Defendants had they known that Defendants would not safeguard their PII as promised or provide timely notice of

a data breach.

199. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendants.

200. Defendants breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' PII and failing to provide them with timely and accurate notice when their PII was compromised in the Data Breach.

201. The losses and damages Plaintiffs and Class Members sustained (as described above) were the direct and proximate result of Defendants' breaches of its implied contracts with them.

COUNT VIII

Unjust Enrichment

(on behalf of Plaintiffs and Class Members)

202. Plaintiffs repeat and reallege all of the allegations contained above and incorporates the same as if set forth herein at length.

203. This claim is brought in the alternative to Plaintiffs' claims for breach of implied contract.

204. Defendants funds its data security measures entirely from its general revenue, including payments made by Plaintiffs and Class Members.

205. As such, a portion of the payments made by Plaintiffs and Class Members was to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendants.

206. Plaintiffs and Class Members conferred a monetary benefit on Defendants. Specifically, they were charged fees when making a cryptocurrency transaction from Defendants and in so doing provided Defendant with their PII. In exchange, Plaintiffs and Class Members should have received from Defendants the goods and services that were the subject of the transaction and have their PII protected with adequate data security.

207. Defendants knew that Plaintiffs and Class Members conferred a benefit which

Defendants accepted. Defendants profited from these transactions and used the PII of Plaintiffs and Class Members for business purposes.

208. In particular, Defendants enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII and instead directing those funds to its own profit. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' decision to prioritize its own profits over the requisite security.

209. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

210. Defendants failed to secure Plaintiffs' and Class Members' PII and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

211. Plaintiffs and the Class have no adequate remedy at law.

212. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiffs and Class Members of the Class conferred on it.

213. Defendants should be compelled to disgorge into a common fund or constructive trust for the benefit of Plaintiffs and Class Members proceeds that it unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiffs and the Class overpaid, plus attorneys' fees, costs, and interest thereon.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

a. For an Order certifying this action as a Class action and appointing Plaintiffs as Class Representatives and their counsel as Class Counsel;

b. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the classes as requested herein, appointing one of the undersigned as Class Counsel, and finding that Plaintiffs are proper representatives of the Classes requested herein;

c. Judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, attorney's fees, statutory costs, and such other and further relief as is just and proper;

d. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

e. An order requiring Defendants to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiffs and the Classes awarding them pre-judgment and post judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Respectfully Submitted,

DATED: April 5, 2024

By: E. Samuel Geisler
E. Samuel Geisler (Ill. Bar No. 6305996)
sgeisler@awkolaw.com
Bryan F. Aylstock
baylstock@awkolaw.com
AYLSTOCK, WITKIN, KREIS & OVERHOLTZ, PLLC
17 East Main Street, Suite 200
Pensacola, FL 32502
Telephone: (850) 202-1010
Facsimile: (850) 916-7449

BRADLEY/GROMBACHER LLP
Kiley L. Grombacher, Esq.
kgrombacher@bradleygrombacher.com
Fernando Valle, Jr, Esq.
fvalle@bradleygrombacher.com
31365 Oak Crest Drive, Suite 240
Westlake Village, CA 91361

Attorneys for Plaintiffs and the Proposed Class